修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報理工　学研究科　総合情報学　専攻　博士前期課程		
氏　　名	松田 和也	学籍番号	1030087
論 文 題 目	より強い Key-Privacy 性を満たすプロキシ再暗号化方式の提案		

要　旨

プロキシ再暗号化方式（Proxy Re-Encryption，PRE）とは Blaze らによって提案された，公開鍵暗号方式の拡張である．PRE では，ユーザ A は自身宛ての暗号文をユーザ B 宛てに変更するための再暗号化鍵を作成し，プロキシと呼ばれる第三者に預ける．プロキシは，この再暗号化鍵を用いてユーザ A 宛ての暗号文を復号することなくユーザ B 宛てに変更できる．

2009 年，Ateniese らにより PRE の Key-Privacy 性が定式化され，その安全性を満たす PRE が提案された．Ateniese らの提案方式は，同じユーザ間の再暗号化鍵を 2 つ用いることにより，片方のユーザを特定できることが指摘されていたが，解決法などは示されていなかった．

また，PRE には ID ベース暗号に再暗号化の機能を加えた ID ベースプロキシ再暗号化方式(Identity-Based Proxy Re-Encryption, IB-PRE)が Green らによって提案されているが, IB-PRE では Key-Privacy 性を満たす方式は存在しない．

本研究では，Ateniese らの方式への攻撃も考慮に入れた従来の Key-Privacy 性より強化された Key-Privacy 性を定義し，強化された Key-Privacy 性を証明可能な PRE を提案する．また，IB-PRE の Key-Privacy 性を定式化し，Key-Privacy 性を満たす IB-PRE も提案する．提案する PRE は，Ateniese らの方式と比べ，再暗号化鍵が大きくなるものの，暗号文長は変わらず，同じ計算量仮定の下でより強い Key-Privacy 性を証明可能である．また，提案する IB-PRE は，Green らの方式と比べ，再暗号化鍵が大きくなるものの．暗号文長は変わらず，同じ計算量仮定の下で Key-Privacy 性を証明可能である．